

CSO

B U S I N E S S R I S K L E A D E R S H I P

Faces, Booked
Guessing SSNs
from profile photos
PAGE 26

**Great
Measurements**
10 identity-
management
metrics worth using
PAGE 30

EVERYONE'S A WINNER?

The ninth annual
**Global State
of Information
Security Survey**
finds tech leaders
brimming with
unwarranted
confidence

PAGE 22



Thinking about migrating to System z? You're in good company.

Since the start of 2010, more than 250 companies around the world have migrated workloads (including Oracle® workloads) to System z. Why? Maybe it's the savings (up to 50% on applicable IT costs). Or the top-rated EAL5 security classification. Or because it delivers up to 99.999% availability and uptime. Or maybe it's an even better reason: all of the above.

ibm.com/facts

IT COST SAVINGS reflect consolidation of software, hardware, maintenance, and other IT costs, hardware and software management over a period of 3-5 years, when consolidating workloads from other systems to a virtualized Linux environment on System z. AVAILABILITY percentage is based on System z servers in a Parallel Sysplex environment, assuming application data sharing across multiple servers. Actual environment, needs, and performance characteristics will vary depending on individual client configurations and conditions. Contact IBM to see what we can do for you. Current as of 7/7/2011. IBM, the IBM logo, ibm.com, System z, Oracle, Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml. © International Business Machines Corporation 2011.

Contents

October 2011 Vol. 10, No. 8

Features...

22 Are You an IT Security Leader?

Cover Story | 2010 Global Security Survey

An astonishing number of survey respondents believe they are IT security leaders. But what does it really take to be a leader, and how does your organization stack up? *By George V. Hulme*

26 Facial Recognition and Social Media Meet in the Shadows

Social Networking Starting with just a Facebook profile photo, researchers obtain partial Social Security numbers and other sensitive information. *Richard Power interviews Alessandro Acquisti.*



Also Inside...

2 From the Editor

4 From the Publisher

8 Join the Discussion

CSOs can catch up on the current state of the law concerning employees' social media usage; Chad McDonald finds a valuable defense course is more like Home Alone than martial arts

11 Briefing

- RSA Spearphish Attack May Have Hit U.S. Defense Organizations
- Are Web Paths Personal Data, Legally Speaking?
- Salted Hash: Security Horror Show
- Hospital Investigates Massive Patient Data Leak



18 Generation Next

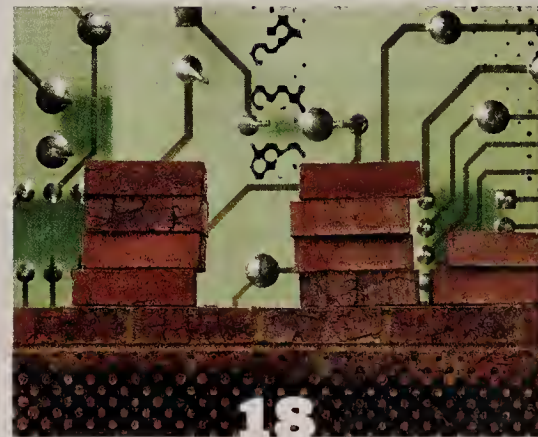
Toolbox Next-generation firewalls may control applications and cost, but don't get sucked in by the hype *By Neil Roiter*

30 Top 10 Identity-Management Metrics that Matter

Industry View *By Frank Villavicencio, EVP, Identropy*

32 Welcome to UltraCorp

Debriefing A few friendly reminders from Team Security for the recent college grads in our workforce



CSO (ISSN 1540-904X) is published monthly except for a combined issue in July/August and December/January by CXO Media Inc., 492 Old Connecticut Path, P.O. Box 9208, Framingham, MA 01701-9208. Periodical Postage Rate at Framingham, MA 01701, and at additional mailing offices. Canadian Publications Mail agreement number 1902075. **Canadian Postmaster:** Please return undeliverable copy to P.O. Box 1632, Windsor, ON N9A 7C9. Copyright 2011 by CXO Media Inc. All rights reserved. Reproduction of material appearing in CSO is forbidden without written permission. Permission to photocopy for internal or personal use or the internal or personal use of specific clients is granted by CSO for users through the Copyright Clearance Center, provided that a fee of \$3.50 per copy of the article is paid directly to Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01970. www.copyright.com. Please specify: ISSN 1540-904X. Permission to photocopy does not extend to contributed articles—followed by this symbol: †. Address inquiries to CSO, P.O. Box 3482, Northbrook, IL 60065; 866 354-1125. CSO is free to qualified security executives. To all others the one-year basic rate is \$70 for the United States and Canada, \$95 to foreign countries (payable in U.S. funds only). The single copy price is \$9 to the U.S. and Canada and \$15 International. Please allow four to six weeks for new subscriptions to begin. Change of Address: Go to www.amedia.com/custsrv/cso and follow the online instructions. **Postmaster:** Send change of address to: CSO, P.O. Box 3482, Northbrook, IL 60065. Printed in the USA.

[FROM THE EDITOR]

To Lead or to Follow?

Is it really best to be on the leading edge? Or is it better to be a fast follower? (Note: If that's your strategy, make sure you really are fast.)

This is an age-old strategy question relevant to a wide array of markets. And it's equally relevant to security professionals, in the contexts of both their organizations and their own careers.

Let's define leading-edge security pros as those who try relatively untested ideas, tools, approaches.

On the plus side, this strategy may provide your company with a competitive advantage in your industry. It can give you a better ability to work with your vendors to help shape products and services that meet your specific needs and priorities. It may offer you more creative and stimulating work, and the ability to retain creative staffers.

The obvious downside of a leading-edge approach is that you will spend time and money on ideas that don't pan out. You and your ideas are an easy target for criticism, and that criticism won't always be unwarranted. Some of your ideas may be simply wrong.

So leading-edgers tend to get either the glory or the pink slip. You have to decide two things: One, are you confident enough in your new ideas to bet the farm? And two, does your risk appetite match that of your organization?

While most of us make those decisions based on our individual situations, there is also a macro question to be addressed. Namely, without risk takers, how can the entire profession move forward?

This question—whether to be on the leading edge or hang back as a fast follower—is important to me in my job, as I set the editorial strategies for *CSO* magazine and CSOonline.com (and those strategies are related but not the same). Should we simply run security news and product announcements? You can make a profitable business that way, and most do. Or should we aspire to something more? Personally, I think reactive security coverage is important, but ultimately it doesn't move the profession forward.

To keep up with the rapid evolution in the attack space, I think the defenders need to continually examine new strategic ideas, processes and organizational models.



I hope you find that *CSO* contributes to that process. In the online version of this column (<http://www.csoonline.com/article/689914>) I'll link to some articles where I believe we've done exactly that.

—Derek Slater, dslater@cxo.com

CSO

Editor in Chief Derek Slater

Senior Editors

Bill Brenner, Joan Goodchild

Copy Editor

Colleen Barry

Editorial Administrator

Pat Josefek

Contributors

Jennifer Baker, George V. Hulme,

Robert McMillan, Richard Power,

Neil Roiter, Jaikumar Vijayan,

Frank Villavicencio

DESIGN

Executive Director, Art and Design

Mary Lester

Art Director Steve Traynor

RESEARCH

Research Manager Carolyn Johnson

TECHNICAL ADVISORY BOARD

Jason Cowling

Jeremiah Grossman, WhiteHat Security

Frank Murphy, TBG Security

Stephen Northcutt, SANS Institute

Richard Power, Carnegie Mellon CyLab

EDITORIAL/ADVERTISING/

BUSINESS OFFICES

492 Old Connecticut Path,

P.O. Box 9208,

Framingham, MA 01701-9208

Main phone number: 508 872-0080

IDG Enterprise
An IDG Communications Company

INTERNATIONAL DATA GROUP

Chairman of the Board

Patrick J. McGovern

IDG COMMUNICATIONS, INC.

CEO Bob Carrigan

Chief Content Officer

John Gallant

BPA
WORLDWIDE™

Virtual desktops. Adapt to any device. In any environment.

VIRTUAL COMPUTING

An iPad™ or a Droid™. A smartphone or a tablet. A Mac® or a PC.

Now you can deliver virtual desktops that will adapt easily to

any device in any combination. Seamlessly. Simply. Securely.

That's the power of
virtual computing, delivered
by Citrix® XenDesktop®

with FlexCast™

technology.

As computing

evolves, say

yes to the demands of your workforce

and your business. All with complete confidence and

complete control. Virtual computing solutions from Citrix.

Simplicity is power. Citrix.

CITRIX®

Citrix.com/SimplicityIsPower

© 2010 Citrix Systems, Inc. All rights reserved. Simplicity is Power and its stylized treatment, XenDesktop and FlexCast are trademarks and/or registered trademarks of Citrix Systems, Inc. or one of its subsidiaries. iPad and Mac are trademarks and/or registered trademarks of Apple, Inc. Droid is a trademark of Lucasfilm Ltd.

[FROM THE PUBLISHER]



Storm Brewing

This summer I embarked on my annual vacation with my wife and daughter. As usual, we spent a day packing the ever-present SUV with what looked like three months worth of supplies and headed to a favorite island of ours for a week of relaxation.

I always cherish this week as a way to get away from the world of security. I get to stay in one place for a week. I get to read. There's no missed flights or TSA screenings. No rental cars or meals on the fly. No conference calls. And, to the guarded chagrin of my wife, only an occasional peek at email.

I've followed this routine for many years with only a few exceptions. I'm the kind of person who embraces routine for the comfort it brings. But this year was different.

We still went to the beach nearly every day. Dined at some great restaurants. Drank far too much. But this year's vacation included an event I really did not plan for when I booked the trip last fall: Irene. As our vacation neared and our anticipation grew, so did the news coverage of Hurricane Irene, whose path was quickly converging with ours.

Now, I've lived through my share of tropical storms and hurricanes over the years. It's a given when you live in coastal New England. We learned young to make a beeline for the supermarket to stock up on bread, milk and batteries—those staples are drilled into every child's head growing up in New England. (When you reach adulthood, you learn that you are also supposed to stock up on booze.)

We were certainly never told to get on a boat, go to an island, and ride out the storm.

As it turned out, Irene (at least on our island) was a bit of a bust. Lots of wind, a little rain, plenty of Dark 'n' Stormy cocktails (recipe for that concoction available upon request). The sun was even out for most of it.

But watching the way people got ready for Irene was a great study of human nature. Some people prepared with the determination of Patton's army, leaving nothing to chance: windows taped, supplies stocked, boats pulled out of the harbor, insurance paid up, wills updated. Others bought a case of beer and threw a party.

If that's not a great metaphor for the differing approaches businesses take to dealing with risk, I don't know what is. Some watch the horizon and prepare for everything that can hurt them. Some sit back, certain in their belief that it will all be OK.

And most of the time everything is OK, but every now and then that person with the case of beer is swept out to sea. And sometimes the person who diligently stocked up and



prepared for the worst actually has to face the worst.

But most times not. As a security professional, your job is to be a little bit of each type: Stock up and prepare...but also buy that case of beer and hope for the best.

—Bob Bragdon, bbragdon@cxo.com

President and CEO
Michael Friedenberg
Group Publisher Bob Melk
Publisher Bob Bragdon
Senior National Sales Manager
Per Melker
East Coast Regional Director, Integrated Sales
Roz Burke
West Coast Regional Director, Integrated Sales
Michelle McHugh
Sales Associate
Sarah Nadeau

INTEGRATED MEDIA AND ONLINE SALES

SVP, GM, Online Operations
Gregg Pinsky
SVP, Online Sales
Brian Glynn
East Coast Online Regional Sales Manager
Richard Hartman
West Coast Online Regional Sales Manager
Erika Karr
Central Online Regional Sales Manager
Stacy Bryne
Director, Online Account Services
Danielle Tetreault

CUSTOM SOLUTIONS GROUP

Vice President Charles Lee
National Sales Directors
Brett Ferry, Karen Wilde

PRODUCTION

VP/Manufacturing Chris Cuoco
Production Manager Heidi Broadley

EXECUTIVE PROGRAMS

SVP, Executive Programs
Ellen Daly
Sr. Director, Event Operations
Deb Begreen
VP, Content Development & Events
Derek Hulitzky

MARKETING

Vice President, Marketing
Sue Yanovitch
Marketing & PR Manager
Lynn Holmlund

LIST SERVICES

Contact Steve Tozeski of
IDG List Services at 508 820-8106 or
stozeski@idglist.com

REPRINTS & PERMISSIONS

For information about reprints and copyright permissions, please contact
The YGS Group, 800-290-5460, ext. 100,
cso@theygsgroup.com

Advertiser Index

ASSA ABLOY..... 10
Avigilon C4
Box..... 31
CA..... C3

Citrix Systems Inc. 3
Hewlett-Packard
Development Co., LP. 13, 15
HID Corp. 5
IBM Corp. C2

Symantec Corp. 17
University of Maryland
University College 29
VeriSign Authentication
Services 6

The object
is Portable,
Flexible and
More Secure.

Introducing iCLASS® SE™,
enabled with the Secure
Identity Object
(SIO) model.



Introducing the next generation of access
control. The platform that simplifies everything.



Learn about SIO.
hidglobal.com/sio
or scan this with
a QR reader



iCLASS® SE™ protects the integrity of your identities, regardless of the card platform. It's also amazingly flexible — use multiple form factors with an access control solution to create your ideal product today, then change it down the road as your business needs evolve by simply reprogramming it.

Powerful, adaptable and designed to be energy efficient, iCLASS SE is truly the next generation in access control. For more information, visit hidglobal.com/secure-CSO



WWW.



VERISIGN™

THE WORLD IS CONNECTING BETWEEN THE DOTS.

Whether you're sharing, remembering, streaming or uploading, the Web is where we connect and experience the world. That's

A photograph of a person at a concert, holding up a smartphone to take a picture. The background is dark with out-of-focus stage lights in various colors (red, yellow, blue). The person's hand and the phone are in the foreground, slightly out of focus. The phone's screen shows a bright, colorful scene, likely the stage. Overlaid on the right side of the image is a white, trapezoidal shape containing the text ".com" in a bold, blue, sans-serif font.

.com

why it's so important that it's available 100% of the time. For more than a decade, Verisign has helped make this possible. It's our experience and infrastructure that keep sites like .com and .net connected and protected. After all, we don't make the world possible, we just make it possible online. See how we keep you connecting at VerisignInc.com/connect.

© 2011 VeriSign, Inc. All rights reserved. VERISIGN; the Verisign logo; and other trademarks, service marks and Verisign designs are registered or unregistered trademarks of VeriSign, Inc., and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.

Join the DISCUSSION

What's on your mind? Security leaders discuss
and debate at www.csoonline.com



BLOG POST

Labor Board Issues Memo on Social Media Cases

CSOs can catch up on the current state of the law concerning employees' social media usage

Realizing the confusion in the area of employee use of social media, the acting general counsel of the National Labor Relations Board issued a memo in August discussing the current state of the law. The introduction provides the reasoning for the memo:

"This report presents recent case developments arising in the context of today's social media. Social media include various

online technology tools that enable people to communicate easily via the internet to share information and resources. These tools can encompass text, audio, video, images, podcasts, and other multimedia communications. Recent developments in the Office of the General Counsel have presented emerging issues concerning the protected and/or concerted nature of employees' Facebook and Twitter postings, the coercive impact of a union's Facebook and YouTube postings, and the lawfulness of employers' social media policies and rules. This report discusses these cases, as well as a recent case involving an employer's policy restricting employee contacts with the media. All of these cases were decided upon a request for advice from a Regional Director."

Businesses have been struggling with developing policies and approaches to the issues presented by social media in the workplace. For those businesses, this report is required reading. It provides one-stop shopping for the current state of

the law in this area. The complete report can be found at: <https://www.nlr.gov/news/acting-general-counsel-releases-report-social-media-cases>.

—Michael Overly

BLOG POST

John Strand Slapped Me in the Face

Chad McDonald finds a valuable defense course is more like *Home Alone* than martial arts

I recently had the opportunity to participate in a course entitled "Offensive Countermeasures," taught by John Strand of PaulDotCom. It was my belief going into the class that I would be honing some "leet skillz" to beat back the attackers persistently targeting the resources that I was hired to protect. I envisioned an electronic Daniel Larusso learning some mystical techniques to fend off the digital Cobra Kai. Far from my fantasy of a cyber Karate Kid, the course is more aligned with *Home Alone*.

Your first impression may be that my *Home Alone* comparison is a slight against either John or the course itself. After all, which would you rather have in your corner: a highly trained martial artist or a mischievous 8-year-old? But for me, this was perhaps the most thought-provoking course that I've had the luxury of attending in my 16 or so years in technology.

We've all been taught that a weakness in antivirus software and intrusion-detection systems (IDS) is their dependence on sig-



natures. These signatures mean that there must be an identified pattern in the mechanisms that an attacker is using against your network. This reliance on signatures leaves us blind to unique attacks. If the bad guys are bashing in your front door in a new and novel way, you won't even know about it until they get in. We know this is a weakness and that our failure to look for unique attacks leaves us vulnerable to one-off attacks.

We know this, yet when we architect our layered security, we all do the same thing. We are all using a firewall, intrusion-protection systems, IDS, antivirus, and so on. We're all using them the same way, yet we're shocked when someone bypasses them. We know that we need to look for novelty in attacks, yet we don't rely on novelty in our defenses. We're relying on boilerplate technology configured in boilerplate ways.

Strand's course, for me, was a wake-up call. I realized that I had fallen victim to vendor speak, expecting that since I was writing big checks for the latest and greatest security technologies and using industry-standard controls, my networks would be safe. I'd sworn nearly a decade ago that I would never get that complacent.

For me, Offensive Countermeasures was more valuable than the tricks and tips in the courseware; it was and remains a catalyst for rethinking how I defend that which I'm responsible for protecting. Don't get me wrong, I got a lot of value from courseware. In fact, I'm working on implement-

ing a few of the items discussed in class. It's just that the moment I realized how complacent I had become was such a slap in the face that I can't place a value on it.

So what is my takeaway from John's class? Aside from the concrete things offered in the courseware, I'm going to look at how I defend my network as if I'm a mischievous 8-year-old. I will find a way to piss off the attackers, slow down their advances, send them on some wild goose chases and find out as much as I can about them in the process. I'll find a way to set traps and alarms, and if I can swing a paint can from a banister, I'll do that too. I plan to spend a lot of time looking at the tools that I have and finding ways to use them in ways unique to my environment so that the bad guys won't be able to follow a standard script to get in. I vow not to make my network a signature or cookie cutter of every other production network out there. I think the message that Offensive Countermeasures offers is something that each of us can take to heart and apply to our own defensive measures: If you choose to ignore John's advice, I'm sure I'll be reading about you in the newspaper soon.

—Chad McDonald

HOW TO REACH US

You can contact us directly or post your thoughts on specific articles and blogs at www.CSOonline.com.

Derek Slater, Editor in Chief

dslater@cxo.com

508 935-4213

Twitter: [@derekslater](https://twitter.com/derekslater)

Bill Brenner, Senior Editor

bbrenner@cxo.com

508 988-7587

Twitter: [@billbrenner70](https://twitter.com/billbrenner70)

Joan Goodchild, Senior Editor

jgoodchild@cxo.com

508 988-7994

Twitter: [@msjoanieg](https://twitter.com/msjoanieg)

Subscriber Services

Phone: 866 354-1125

Fax: 847 564-9453

E-mail: cso@omeda.com

Reprints & Permissions

For information about reprints and copyright permissions, please contact The YGS Group, 800 290-5460, ext. 129, cso@theygsgroup.com.



MORE ON THE WEB

Wake Up With Salted Hash

Your daily security news cuppa joe: CSOonline's new **Salted Hash blog and newsletter** covers the news as it happens.

<http://blogs.csoonline.com/blog/cso>

Access control
isn't one size fits
all either.



Copyright © 2011 ASSA ABLOY Inc. All rights reserved.

From patented key systems to full-featured, online integrated locksets, ASSA ABLOY offers access control solutions tailored to the unique locking needs of each opening. With the industry's largest range of products, from the most trusted brands, your security dollars reach farther into your facility.

Contact your ASSA ABLOY Integrated Solutions Specialist for a consultation on your next project. Visit www.intelligentopenings.com/SecurityContinuum.



Using your mobile phone,
scan this Microsoft® Tag.
Download the free mobile
app at <http://gettag.mobi>

ASSA ABLOY

ADAMS RITE | CORBIN RUSSWIN | HES | MEDECO | NORTON | SARGENT | SECURITRON | YALE

The global leader in
door opening solutions

"There's a gray, squishy line between security and stupidity, and these guys crossed that line some time ago." PAGE 14

Briefing

TRENDS, STATS AND FAST FACTS

Edited by Bill Brenner

PHISHING

RSA Spearphish Attack May Have Hit U.S. Defense Organizations

One attack file was created using a Chinese-language version of Excel

The hackers who in March broke into RSA, the security division of EMC, used the same attack code to try to break into several other companies, including two national security organizations, according to data provided by the malware analysis site VirusTotal.

"According to our data, RSA was just one of the targets," Bernardo Quintero, the founder of VirusTotal, said in an email interview. Attackers "used the same malware to try to penetrate other networks."

VirusTotal is a popular site with security professionals, who use it to get a quick industry consensus on suspicious files. It runs any file through a battery of antivirus-scanning engines and spits out a report within minutes. Someone at EMC used the service on March 19 to analyze an email message that contained the spearphishing attack that was used to break into RSA.

But according to Quintero, before the attack was publicly disclosed in mid-March, the same maliciously encoded Excel spreadsheet had already been uploaded to VirusTotal 16 times by 15 sources.

The file was first uploaded on March 4—the day after the phishing message was sent to RSA—and the malware wasn't detected by any of the site's 42 antivirus engines.

Because it relies on anonymous submissions, VirusTotal won't say who uploaded the documents. But according to Quintero's analysis, two of the targets were entities related to U.S. national security.

Buried in the metadata of the attack files is another clue, a sign that whoever created the attack used a Chinese-language version of Excel: The file was created using Windows Simplified Chinese. The attackers could have deliberately changed the file's settings to make it look like it came from China, but Quintero believes it was a simple



oversight on the part of the hackers.

It would be natural for the person who wrote the RSA attack code to try to use it as much as possible before it was discovered and patched. Here the code was embedded in Excel documents, but the flaw it exploited when the documents were opened actually lay in Adobe's Flash Player.

Adobe learned of the issue on March 9, when a "partner in the security community" noticed the attack code at an undisclosed customer site, says Wiebke Lips, an Adobe spokeswoman. Before Adobe released its first advisory, a second customer—not RSA—also reported the attack, Lips said.

The RSA hackers broke in using a basic social engineering attack. They sent an email that looked like it came from an RSA partner, online recruiting firm Beyond.com, with the simple message, "I forward this file to you for review. Please open and view it." That file was named "2011 Recruitment plan.xls." Quintero says the hackers also used a second file name, "survey-questions_2011.xls."

In a post written shortly after the Adobe flaw was first disclosed, the Contagio Malware Dump blog listed four Excel files that were being used in attacks, including a "Nuclear Radiation Exposure and Vulnerability Matrix.xls" file that was doctored to look as though it came from the Nuclear Regulatory Commission.

(continued on next page)



(continued from previous page)

It's not clear who the message containing the malicious file was addressed to, but in the March 17 spearphishing email that the Contagio blog also published, the attackers seem to be going after someone who would have taken an interest in the recent Japan earthquake.

Headed by the subject line "Japan Nuclear Radiation Leakage and Vulnerability Analysis," the email says, "The team has poured in heart and full dedication into this. Would be grateful if you appreciate it."

VirusTotal's findings offer clues but no answers to the questions raised by the attack on RSA, which was ultimately seen as a stepping stone to further attacks on defense contractors Lockheed Martin, L-3 and Northrop Grumman.

It's possible that the hackers who developed the attack used on RSA shopped their attack code around to other groups with other goals. Once hackers discover a previously unknown zero-day flaw, there's a lot of pressure to exploit it as much as possible before it is made public and then patched, says Alex Stamos, a founder of NCC Group's iSec Partners.

So it's not at all shocking that other companies were targeted with the same attack code, he says.

McAfee's research shows that other defense organizations were targeted by the attack, although not necessarily at the same time as the RSA incident, says Dmitri Alperovitch, McAfee's vice president of threat research.

"After that vulnerability became known, a lot of people started leveraging it, and that continued through April," he explains.

—Robert McMillan

PRIVACY

Are Web Paths Personal Data, Legally Speaking?

The behavioral advertising industry says no, but a consumer-advocacy group is petitioning lawmakers not to accept this argument

A leading international consumer group has called on the U.S. Federal Trade Commission and the European Union's main body for data protection, the Article 29 Working Group, to reject requests that behavioral advertising companies—online advertisers that track users to serve up personalized ads—be allowed to regulate themselves.

In a letter to lawmakers, the Transatlantic Consumer Dialogue (TACD) group said it was deeply concerned about the EU position on how Internet users are tracked online and how their data can be sold on to advertisers.

The group, which represents Internet users' interests, is alarmed at moves by the advertising industry to have Internet users' Web paths defined as "non-personal data."

"The EU should not accept the advertising industry's attempts to redefine people's Internet usage as 'non-personal data.' It's certainly personal, and a clear line should be drawn as this billion-dollar industry is now the currency of the Digital Age," says Monique Goyens, director general of the BEUC, a European consumer-advocacy organization.

The self-regulation system uses an icon to provide notice of data-collection practices, but TACD says that research shows very few users ever click on it.

"The current icon program gives a false impression of fairness," Goyens says.

Julian Knott, coordinator of the TACD secretariat, said in a letter, "The icon is the foundation of what's supposed to be a robust program of 'best' practices that can effectively empower users to make critical choices about their online privacy. Consumers who may click on the icon are initially dissuaded from taking appropriate measures to safeguard their privacy, as they confront an array of information that online profiling is primarily about providing them with 'appropriate'

advertising, is non-personal and supports their access to a 'free' Internet."

"Under both the EU and U.S. self-regulatory regimes, sensitive data, such as that involving consumers' health or finances, can be collected without ensuring that they have real opportunities to proactively protect how such information is used," Knott said.

Behavioral advertising collects information primarily by using cookies, tiny pieces of code installed on the user's computer to remember preferences relating to a particular website.

The law governing cookies in the EU is the revised ePrivacy Directive, which became law in May and requires companies to obtain explicit consent from Web users before tagging them with cookies.

However, the vast majority of EU member states failed to implement the law, citing confusion about how to define "explicit consent."

The European Commission recently started legal action against the 20 countries that failed to implement the new rules.

—Jennifer Baker



VIEWPOINT

**Tom Reilly**

VP AND GENERAL MANAGER
HP ENTERPRISE SECURITY

Tom Reilly has served as vice president and general manager of HP Security Solutions since October 2010. He was previously CEO and president of ArcSight, Inc.

FOR MORE INFORMATION:
www.hpenterprisesecurity.com

Security: A Transformational Approach to Combating Cyber Threats

As new security threats appear, CIOs are increasingly challenged with keeping their organizations safe from cyber attacks. Find out from HP's enterprise security lead how to get out from behind the eight ball.

How are evolving IT environments—mobility, IT consumerization, virtualization, cloud computing—impacting today's security landscape?

Major transitions in IT inevitably lead to opportunities for cyber criminals. We're now seeing the use of cloud computing, mobility and social media greatly expand the threat surface for organizations to defend, especially against attacks that target users and Web applications. All of these technology trends provide valuable benefits, but organizations need to think about new security controls to offset the associated risks.

Are companies who don't take a proactive approach to neutralizing potential security risks in danger of being left behind, or worse, attacked more easily?

We think security needs to move from a defensive position to a more proactive, risk-management approach. This includes identifying critical IT services that support sensitive data and understanding where the vulnerabilities lie within each of those systems and applications. It's more effective for enterprises to anticipate, close up, and protect vulnerabilities in advance rather than locking systems down and reacting after a breach has occurred.

What do your research groups tell you are the newest wave of security threats facing enterprises today?

Cyber threats have become more sophisticated, persistent and unpredictable. New research commissioned by HP found that the volume, cost and complexity of security threats have continued to escalate. One recent survey found more than 50 percent

of executives believe that breaches in their organizations have increased, with another study revealing that the cost of cyber crime has risen 56 percent per organization on an annual basis. While there is increased awareness, cyber-criminals continue to find more surface vectors and increased opportunities for attacks.

Will the point products that handle security breaches today become ineffective in mitigating the types of security threats we'll be seeing in the future?

There are thousands of security vendors with very good point products; however, the information generated by a single security product does not provide a complete picture. Information security teams must deliver actionable intelligence to their organizations to minimize risk through the correlation of not only security information, but also the functions of security technologies. Unless the right data can be brought together intelligently and security products can work together intelligently, we'll continue to be on our back foot when it comes to fighting cyber crime.

Explain for us how HP's new security ecosystem can provide diverse enterprise security coverage.

To help organizations manage the risk and compliance demands associated with escalating IT complexity and security threats, HP has established a foundation for a unified approach to enterprise security. The HP Security Intelligence and Risk Management (SIRM) platform offers advanced correlation, application protection, and network defense technology to protect applications and IT infrastructures from sophisticated cyber threats. Supported by an expansive network of partners, the platform helps to remove risk from existing infrastructures and establishes a framework for deploying future systems within a more secure environment.





SALTED HASH

SALTED HASH

Security Horror Show

PEOPLE LOVE to complain about the TSA and the body scans they now suffer through during airport security screenings. We know that—misguided or not—the goal is to stop terrorists from hijacking planes.

But if you stop a middle-aged woman and tell her she can't enter the United States because the cops went to her home after an attempted suicide years ago and that makes her a security risk, well... What is there to say? It's painfully obvious that some in airport security are sitting on their brains.

It's reasonable to argue that body scans and enhanced pat-downs are over the line. But denying people entry to the country because of incidents like this just goes to show how flawed this system is.

Security experts have a name for measures that amount to window dressing: security theater. I call this a security horror show.

Here's an excerpt from the CBC News article that set me off:

"More than a dozen Canadians have told the Psychiatric Patient Advocate Office in Toronto within the past year that they were blocked from entering the United States after their records of mental illness were shared with the U.S. Department of Homeland Security.

"Lois Kamenitz, 65, of Toronto, contacted the office last fall, after U.S. customs officials at Pearson International Airport prevented her from boarding a flight to Los Angeles on the basis of her suicide attempt four years earlier.

"Kamenitz says she was stopped at customs after showing her passport and asked to go to a secondary screening.

"There, a Customs and Border Protection officer told Kamenitz that he had information that police had been to her home in 2006.

"I was really perturbed," Kamenitz says. 'I couldn't figure out what he meant. And then it dawned on me that he

was referring to the 911 call my partner made when I attempted suicide.'

"Kamenitz says she asked the officer how he had obtained her medical records.

"That was the only thing I could think of,' she says. 'But he said, no, he didn't have my medical records but he did have a contact note from the police that [they] had attended my home.'

"Stanley Stylianos, program manager at the Psychiatric Patient Advocate Office, says his organization has heard more than a dozen stories similar to Kamenitz's."

When the police visit your home because you tried to kill yourself, it's a tragic situation. But it's a medical emergency, not an attempt at murder. It's certainly not an attempted terrorist attack.

If this doesn't outrage security professionals and privacy advocates everywhere, then maybe I have lost my touch. A decade after 9/11, I have to ask if this is really the best we can do.

There's not much more to say about this, other than that it's time for DHS to seriously reconsider its procedures.

There's a gray, squishy line between security and stupidity, and these guys crossed that line some time ago.

—Bill Brenner



CSOonline's new Salted Hash blog and newsletter covers the news as it happens: blogs.csoonline.com/blog/cso

Security Wisdom Watch



Thumbs down: 9/11 anniversary hacks: Hackers used the 9/11 anniversary to create online mischief, hijacking NBC News's Twitter account and posting bogus updates about an attack on New York. As a CNN reporter said on that day 10 years ago, "There are no words."



Thumbs both ways: Car hacking: Some vendors are stirring the FUD pot with warnings about hackers hijacking increasingly computerized cars. It's a bit early for this to be a real threat. But as we've seen with smartphone hacking, theory eventually becomes reality.



Thumbs down: Airport screening: Telling a woman she can't enter the United States because the cops went to her home after an attempted suicide six years ago is not going to reduce terrorism. So why are customs officials doing it? In our view, it's security theater gone horribly wrong.



Thumbs up: Social media in emergencies: Twitter, Facebook and other social media have proved valuable during recent earthquakes and hurricanes. If these platforms existed on 9/11, additional lives might have been saved.



Thumbs both ways: Sourcefire's Agile Security: The vendor is taking care to avoid compromising its Snort open-source intrusion-detection system while it expands its portfolio. This as a big relief, as many organizations rely on Snort. Merging new technology with old can be problematic, but it's so far, so good during Sourcefire's recent steady expansion. —B.B.



CYBER THREATS. MOBILITY. CLOUD. SOCIAL MEDIA.

INTRODUCING MORE THAN JUST A LITTLE RISK TO YOUR BUSINESS?

HP Enterprise Security has what you need to secure your applications, information and operations. Backed by our unparalleled security research team, we can help you protect your enterprise and identify risks before you even know they exist.

For more information go to
www.hpenterprisesecurity.com.



DATA BREACH

HOSPITAL INVESTIGATES MASSIVE PATIENT DATA LEAK

Confidential medical data of up to 20,000 patients may have been compromised

Stanford University Hospital in Palo Alto, Calif., is investigating how a spreadsheet containing personal medical data on 20,000 patients ended up being publicly available for nearly a year on a homework help site for students.

The spreadsheet first became available on the site in September of last year as an attachment to a question supposedly posed by a student on Student of Fortune, a website that lets students solicit help with their homework for a fee. The poster asked how the medical data in the attachment could be presented as a bar graph.

The spreadsheet was being handled by one of the hospital's billing contractors and contained names, diagnosis codes, account numbers, and admission and discharge dates for about 20,000 patients who visited the emergency room at the hospital in 2009. No Social Security numbers, addresses, birth dates, or credit card details were compromised in the breach. Even so, Stanford has agreed to pay for identity theft monitoring services for the victims.

The hospital learned about the spreadsheet in August, when a patient noticed it on the Student of Fortune website and informed the hospital about it. The spreadsheet was taken down immediately after.

Stanford has since suspended its relationship with the billing contractor and has asked it to either destroy or securely

return all data about Stanford patients that it has in its possession, the *New York Times* quoted a hospital spokesman as saying. The spreadsheet had been prepared by the contractor as part of a billing analysis for the hospital.

Student of Fortune did not immediately respond to a request for comment on the incident. But a spokeswoman for

the homework-help site is quoted in the *New York Times* as saying that the site had been unaware of the data until it was informed about it by the hospital, at which time it promptly took the information down. The spokeswoman says the identity of the poster cannot be determined.

This is the second time in less than two years that Stanford has been in the news over a data breach. In January 2010, an employee stole a computer containing protected the health information of 532 patients from the hospital's heart center.

The breach resulted in the hospital getting hit with a stiff \$250,000 fine by the

California Department of Public Health for its alleged failure to notify affected victims of the breach as soon as was required under state laws. Stanford has appealed the fine, contending that it acted in a manner consistent with the state's data breach reporting requirements.

The breach shows yet again how ineffective HIPAA has been in getting organizations that handle healthcare data to take better care of it, says Deborah Peel, founder and chairman of the Patient Privacy Rights Foundation.

Much of the problem stems from the indiscriminate sharing of sensitive personal information among "legions of secondary users," she says.

The average hospital has between 200 and 300 outside vendors and partners with access to patient data, Peel says. "We do not have an effective federal health privacy law. HIPAA was gutted in 2002, when control over who can see and use patient data for all routine uses was eliminated," she says.

The only way to really get a grip on the problem is to allow patients to exert more control over who has access to their data. "Data should be used for a single purpose after the patient gives consent, such as consent to use the data to pay a claim or send to a consultant. Consent should be obtained for any secondary or new uses of data," she says.

—Jaikumar Vijayan

"We do not have an effective federal health privacy law. HIPAA was gutted in 2002."

—DEBORAH PEEL, FOUNDER AND CHAIRMAN OF THE PATIENT PRIVACY RIGHTS FOUNDATION



Mobility: Where Security and the Cloud Come Together

In the ongoing struggle between employees who want to use their mobile devices to access corporate data and IT departments that strive to secure and control all endpoints, the employees are winning.

As companies attempt to keep up with the pace of business today and compete in the global marketplace, employees are demanding access to corporate networks and data from wherever they may be, with whichever device they're using. Business units are putting pressure on IT to comply with regulatory requirements. Now the challenge lies in finding ways to secure and manage mobile workers without interfering with how they get their jobs done.

However, in a recent IDG Research Services study of 115 IT security professionals, 59 percent of the respondents reported that they are just somewhat or not at all effective at minimizing mobile security and compliance risks. Security professionals are well aware of the risks: 94 percent of the respondents believe that there is at least a moderate amount of risk inherent in supporting a mobile workforce, including unauthorized data sharing, data loss, and the introduction of malware to the corporate LAN.

So IT departments need solutions to protect mobile assets—particularly notebooks, which are still the most prevalent mobile computing devices and often contain sensitive or confidential information. Once these devices leave the corporate office, they become potential threat vectors that can lead to data breaches.

Not only are mobile devices at relatively high risk but studies also show that employee behavior changes when the employees aren't in the office. For example, employees are 35 percent more likely to violate corporate Web surfing policies outside of the office than when they are in the office. Also, most corporations haven't updated their acceptable-use or compliance policies for assets used outside of the office.

Finding Balance

Cloud-based services are emerging as effective alternatives that help enterprises strike a balance between

flexibility and protection without requiring significant up-front investments or creating drains on IT resources. These solutions provide data security for mobile users in a way that has the least impact on corporate networks, can be quickly and easily implemented and can scale as the mobile workforce grows.

For comprehensive security of Windows-based notebooks, Symantec Endpoint Protection.cloud protects mobile devices without having an impact on the end user experience or requiring the installation of additional hardware or management software. The service provides advanced technologies for antivirus and antispyware efforts, firewalls and host intrusion prevention to protect notebooks, whether in the office or on the road.

Because the Web is a primary threat vector, Symantec also offers a service to help enterprises implement acceptable-use policies for mobile employees, facilitating the same level of protection as for office-based employees. Symantec MessageLabs Web Security.cloud protects mobile users from Web-borne threats via URL filtering and gives IT departments control by monitoring and enforcing Web acceptable-use policies with minimal latency.

To help enterprises maintain compliance with regulations, Symantec offers encryption for laptops, external drives and USB flash drives mobile employees take on the road.

The mobility trend will continue to sweep through enterprises, but security doesn't have to lag behind. Effective cloud-based solutions give IT professionals a scalable, cost-effective way to strike a delicate balance between flexibility and control.

For more information, go to www.csoonline.com/whitepapers/symantecmobile and get a free download of the full white paper "Mitigating Risk in a Mobile World" and the complete research results.



Toolbox

TOOLS, TECHNOLOGIES AND TACTICS

By Neil Roiter

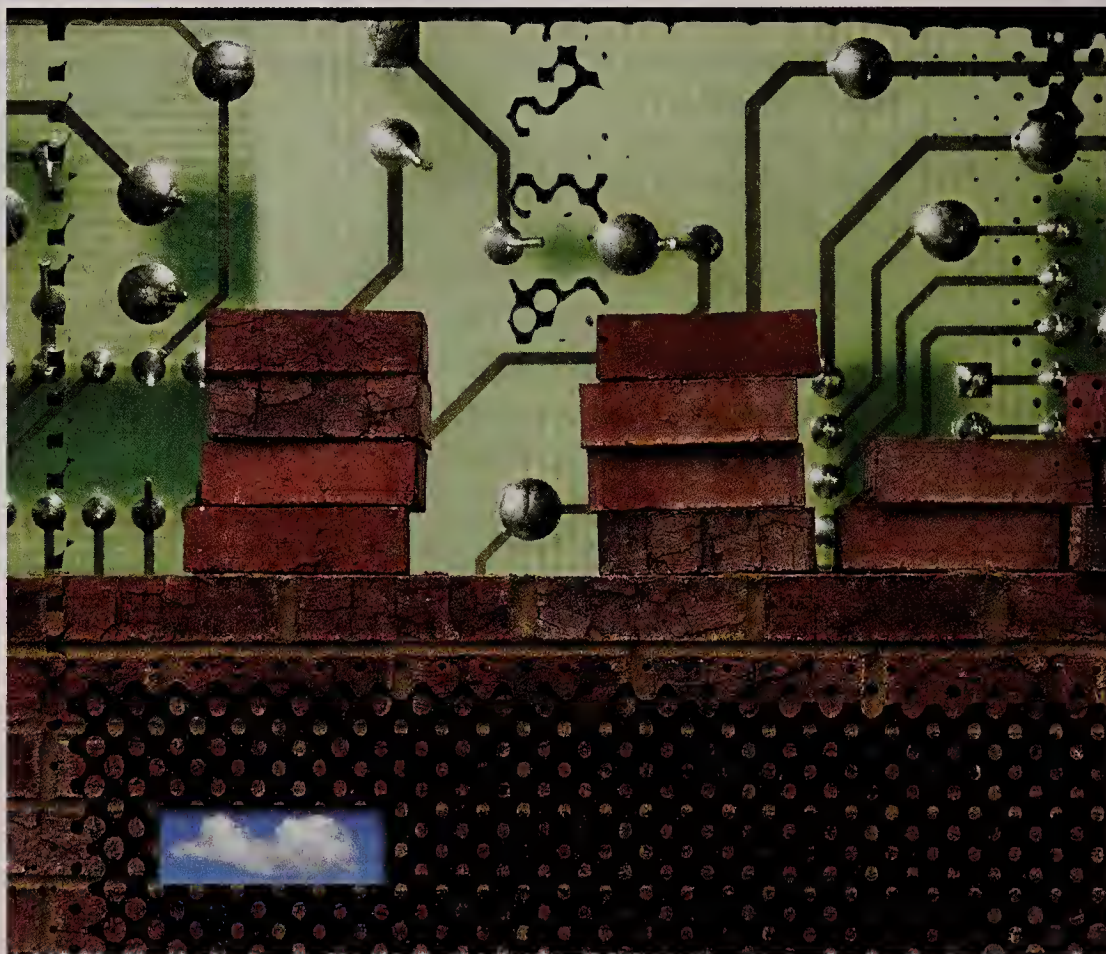
Generation Next

Next-generation firewalls may control applications and cost, but don't get sucked in by the hype

Next-generation firewalls, meet this generation's network and threat environment.

Traditional stateful inspection firewalls, with their port- and protocol-based controls, have limited visibility into the contemporary Web-based network landscape. Thanks to the explosive popularity of Web 2.0, thousands of Web-based business and consumer apps and attacks are launched primarily through the application layer. Stateful inspection firewalls cannot distinguish what applications are passing via http and https over ports 80 and 443. Attackers have become adept at using low-and-slow techniques in targeted attacks that evade intrusion-prevention systems (IPS).

True, next-gen firewalls perform deep packet inspection to identify application traffic at Layer 7, performing a single inspection pass that integrates firewall, intrusion-prevention and additional security capabilities in a single high-performance appliance. Application intelligence, combined with user identity information, provides context for highly granular firewall access rules that allow for detection of contemporary Web-based attacks. Enterprises can enforce security and acceptable-use policies in ways that make sense for the business, in contrast to black-and-white policies like "No one can use Facebook" or



"We have to let everyone use Facebook."

This is a fast-growing market, created when Palo Alto Networks appeared on the scene in 2007 with the capabilities and feature sets that characterize what are now known as next-gen firewalls. Most other firewall and unified threat management vendors have introduced, or are at least developing, network security products that

provide fine-grained application and user controls in integrated, high-performance appliances.

"IPS should have been combined with firewall much sooner," says Greg Young, a Gartner research VP. "IPS ballooned up beyond \$1 billion and took on a life of its own; no one was integrating. Palo Alto [Networks' next-generation firewalls]

changed the game, and incumbent firewall vendors have been forced to react to meet that threat."

Next-gen firewall adoption was between 5 percent and 10 percent of total firewall appliances in 2010, according to a joint report by Infiniti Research and TechNavio Insights, and is expected to gain significant market share over the next few years. Gartner has predicted that next-gen firewalls will comprise 35 percent of the installed firewall base by the end of 2014 and will account for 60 percent of all firewall purchases.

In some cases, enterprises are deploying next-gen in front of their existing network firewalls and IPS to get the benefits of app-layer and user-ID filtering without a wholesale rip-and-replace. In other cases, they put it behind their firewalls and IPS to see what is getting through.

"They look at it as an adjunct," says Lisa Phifer, president of consultancy Core Competence. "They either want to apply extra granularity or use next-gen to act as a sanity check if something goes through that wasn't expected."

But that's now the exception, says Young. Today, 95 percent of next-gen purchases are firewall replacements, as the newer technology has proven its value and the vendor selection has widened.

Driving the Market: Consolidation and Cost Come First

Application-based controls and security provide the flash and the coolness factor, but the business case most often relies on the savings and reduced management overhead that come with consolidating several security products into an integrated platform that meets the needs of highly demanding enterprise networks.

"It became apparent that we could consolidate a lot of the technologies we were looking at," says David Rahbany, director of enterprise IT infrastructure at Hain Celestial Group. Hain purchased and deployed Fortinet next-gen appliances when it consolidated connectivity among its distributed sites and corporate data centers from Internet-based VPN to a multiprotocol label switching (MPLS) network.

"The driver was really the costs associated with the MPLS deployment. 'We could

focus our gateway security perimeter on a handful of sites, for which next-generation products better suited our needs." Rahbany also cited better management control for a relatively small IT staff.

The end of a normal refresh cycle for perimeter devices is a logical time to look at replacement, but a case can be made for off-cycle next-gen deployment if the savings and benefits are compelling. For example, 24-Hour Fitness, a Palo Alto Networks customer, had a year left in the depreciation write-off for its existing firewalls, but found that the savings in purchasing sooner rather than later more than offset the lost depreciation.

Next-gen firewall adoption was between **5 percent and 10 percent of total firewall appliances in 2010**, and is expected to gain significant market share over the next few years.

"It was smarter to combine everything—firewall, malware detection, Web filtering, threat management—at a lower cost," says Jason Kwong, director of IT operations and security. "The justification wasn't hard."

But although consolidation and cost savings are paramount, application awareness and control (what Gartner's Young calls the "sizzle") are a key driver as well. Next-gen appliances enable enterprises to create policies and rules that reflect the modern Web-based IT business environment, including the growing use of Web 2.0 for both business and personal use. Just as significantly, the technology can be used to monitor and enforce compliance with these policies. It also provides the ability to identify thousands of individual applications and establish rules governing not only which are allowed, but under what circumstances and by whom.

So, for example, peer-to-peer applications might be prohibited, but Skype might be authorized for users who have a legitimate business need for it. All users might be allowed to use Facebook to network but might be blocked from accessing the site's applications.

From a security perspective, next-gen

appliances provide much stronger filtering and threat detection than the combination of traditional firewalls, standalone IPS and other security products, such as URL filtering. If the appliance is performing deep packet inspection on the firewall, it can more effectively reduce the traffic to authorized applications and users, and simplify detection of potential attacks by focusing on what still gets through. The single-pass inspection up front allows the product to correlate and analyze various security engines.

"In many ways, this is a call for a better IPS that's aware of protocols and applications," says Rick Moy, president and CEO of

NSS Labs. "Now it's imperative for the firewall to know more about the applications because it has to work in conjunction with IPS to provide context for IPS to do its job."

For example, Moy says, the firewall can tell the IPS module that the application being used is Skype, and the IPS can focus on detecting known Skype attacks rather than applying all of its thousands of signatures to every packet.

"The flip side to enablement is whether I can limit the number of applications that can penetrate the network, thereby controlling avenues of attack," says Chris King, Palo Alto Networks director of product marketing.

This integrated approach makes it easier to track the source of a potential security event than with separate appliances, and effectively reduces the false positives and false negatives associated with IPS.

"We've mitigated risk in providing access to those applications and gained better insight into who's using what and how," says 24-Hour Fitness' Rahbany. "We have management oversight that we lacked. We're in a better position to anticipate threats and manage bandwidth and applications."

Evaluating Next-Gen Tools: What to Look For

Next-gen firewalls are complex products, and vendors claim an impressive array of capabilities. Determining how well an appliance meets your needs requires understanding your enterprise's requirements, and a lot of research and testing.

Look under the hood. All vendors will claim to have a special sauce for doing that voodoo that they say they do so well, but next-gen requires sophisticated software and hardware engineering that didn't exist until a few years ago. Hold the vendor's feet to the fire to get them to explain their software and hardware architecture and how it accomplishes the required processing, inspection, correlation and analysis. Consult third-party reviews and analysis as well. Questions to ask include:

- Is there actually only one inspection pass being leveraged by the various engines in the box?
- Is inspection taking place on the firewall, where it can effectively pre-filter traffic and provide context for IPS and other integrated tools?
- Are the firewall and IPS truly integrated, or simply packed in the same box?
- Does the product run on standard hardware or as a dedicated appliance? The general trend in IT has been toward use of standard hardware, but next-gen requires purpose-built appliances that can meet its demands in an enterprise environment.
- Have they built truly new products or just adapted existing firewall and IPS technology? Most vendors, with the exception of Palo Alto, have existing firewall and IPS engines, and are now trying to integrate application control and other features with the tools they already have, says Young. "They're not completely integrated, so they have this hair-pinning of traffic between modules," he says. "This is highly inefficient."

Check its performance. All this capability comes at a price. Unlike traditional network firewalls, a next-gen appliances (like standalone IPS) is a "bump in the wire" that can clog the flow of production traffic. Connections per second—throughput with all the security features turned on—must be

carefully evaluated and tested in as close to a real-world production environment as possible.

One issue in particular to address with your vendor and in testing is how the next-gen firewall handles encrypted traffic. Can the firewall intercept, decrypt and re-encrypt SSL/TLS, SSH and VPN traffic, and, if it does, at what cost to performance?

Determine realistic requirements for your production environments and test accordingly. Where and how you use the next-gen firewall is a strong factor to consider in assessing performance. Financial transactions, stock trading, and so on, are extremely performance-sensitive. Weigh the criticality of the assets and systems you are protecting when creating appropriate rule sets and deciding which security

not, there are third-party testing providers, many of whom make use of these tools.

"Pilot the heck out of it," says Kwong. "I've dealt with many firewalls, and out-of-box we needed to tune a lot of parameters before we got to the right performance level. From my experience with previous firewalls, I've always found performance didn't quite match the claims."

Be realistic about application control.

Before you are blown away by a vendor's assertion that they have so many thousand applications in their library, consider your application policies and practices. Learn which applications your company's employees are using for legitimate business purposes, which are likely to be used in the future, who is using them and how are they being used. Armed with this information,

All vendors will claim to have a special sauce for doing that voodoo that they say they do so well, **but next-gen requires sophisticated software and hardware engineering** that didn't exist until a few years ago.

services to enable. For example, says NSS Labs' Moy, unified threat management (UTM) performance typically drops by 60 percent from 10Gbps to 3 or 4Gbps when IPS is enabled, and there is an even more drastic reduction, to 300 to 400Mbps, when antivirus capabilities are turned on.

"I'd be skeptical about turning on [antivirus] on the firewall," he says. "In front of the data center, probably not, but maybe at the perimeter."

More and more complex rules will also affect performance, so factor that into your testing.

"The deeper the policies, the more you feel an impact," says Core Competence's Phifer. "As you layer on additional checks, it is going to get slower and slower."

There are a number of high-end products on the market that perform load and security testing. These are expensive, but worth investing in if you are going to be doing a lot of network equipment and network security product testing in-house. If

you can create security and appropriate-use policies and evaluate next-gen firewall products on their ability to monitor and enforce policy around these apps.

"Vendors claiming large numbers of applications is kind of meaningless; the numbers are not important," says Gartner's Young. He recommends that once you decide which applications you want to deal with, you make sure they are in the library, find out whether they produce false negatives or positives, and run them through a configuration exercise.

"If you want to block Mafia Wars or allow Facebook for sales and marketing, how difficult is the task, and does the workflow it produces make sense?" he says. Configuring an application should be easy, and should be done using a wizard-like, hierarchical interface.

Young also suggests testing a topical application that's known to be malicious or cause problems on networks and see if the appliance catches it.

Make sure it's easy to manage. Next-gen firewalls are a different experience from managing traditional firewalls and standalone IPS, so it is critical that the management interface make the transition as seamless as possible. On one hand, the ability to define very specific, context-based rules for applications and users introduces a new level of complexity. On the other hand, the rules can be more sharply defined, so it's easier to get exactly what you intend without ambiguity or layers of rules.

"You can use that granularity and power, but in a way that becomes more manageable," says Phifer. "But it will still be harder than before; it's part of the pain of gaining that extra level of control."

It's important that the management interface and rule creation be as intuitive as possible and reflect the integration of the components' capabilities.

"The ability to centrally manage and distribute policy was a criterion," says Rahbany. "The firewall rule set is very intuitive and familiar. There was some discrepancy between centralized management tools and the UI at the firewalls themselves."

Caveat Emptor

Don't assume anything based on vendor claims. Not every product that's called "next-gen firewall" lives up to that description, and product capabilities vary widely. Take a hard look at:

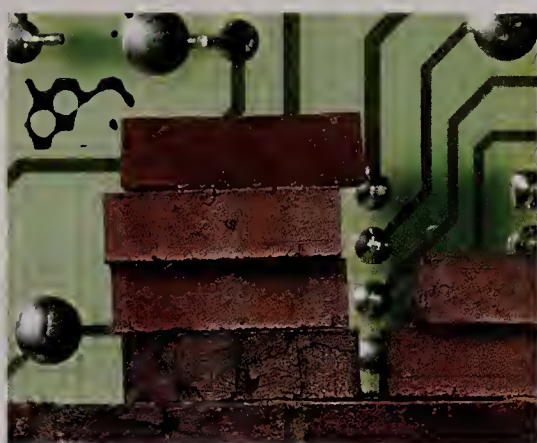
Throughput. What happens when all the security services are enabled? How does the appliance perform under a real-world rule set tailored to your environment?

Detection. Test to determine if the vendor has made trade-offs between performance and detection. IPS has historically been marked by compromises in this area to keep up with high-speed networks.

Integration. Determine whether the components are truly integrated or just colocated. Integrated appliances will perform a single inspection pass on the firewall for all components.

Standard hardware. This is a showstopper. Next-gen firewalls require the muscle of purpose-built hardware. "Beware of people who are overly reliant on general-purpose equipment to deliver all this extra inspection and try to defy the laws of physics," warns Young.

Applications. Vendors are likely to have



a tough time keeping up with every new application and how enterprises will use them. "Despite the fact that vendors all have long lists of applications that they advertise, this is probably where customers might be most disappointed," says Phifer, because it seems like every day some app is being added to Facebook or there is a new capability being added to Twitter. Vendors will constantly be playing catch-up with what everyone is experiencing live.

Dos and Don'ts for Next-Gen Firewalls

DO understand the new management paradigm. Policies and rules are built around applications and users, not just ports and protocols, and will be tightly tied to business practices—authorized and ad hoc—that are very different. However, once the admins get the knack, rule sets will be more streamlined and specific.

"There's a learning curve; you come to deal with terms that are much more human-understandable, using user names and groups instead of IP addresses," says Oded Gonda, vice president of network security at Check Point. "It requires some patience for people used to working in a very network-centric role."

DO have policies controlling application use. Have at least basic application policies that can be translated into rules that take advantage of next-gen capabilities, rather than simply transferring old rules without regard to what you are now able to do. This enables users to productively use applications that may have been banned or severely restricted.

"Organizations that already have a policy, or goals, or a culture of what they can do, will be much more successful," says Young. "I see a lot of dissatisfaction when organizations don't have those policies, [and they]

bring in application control and don't have anything to enforce."

DO consider the incumbent vendor. Retraining and re-creating your rule base can be a major disruption. While next-gen requires some rule changing, there's generally more headaches associated with changing vendors. If you have a major investment in a firewall vendor across a large, distributed enterprise, account for the level of change you're talking about. Young recommends planning for two- and five-year windows with the aim of reducing or eliminating multiple firewall vendors.

DO service branch offices as well as central locations. Next-gen firewalls from the same vendor should be deployed in branch offices. If you have UTM appliances in branch offices, plan on replacing them with appropriately sized appliances as you bring in the next-gen technology. This will allow central management, one-source service and uniform policy administration.

DON'T ignore the value of application visibility. There is considerable value in simply monitoring application and user activity through the next-gen firewall, even if you already have Web application acceptable-use policies in place. You will see activities and application usage that you may have been unaware of, that will help you tweak existing rules or create new rules and policies, and avoid restricting or blocking productive business activity.

"There's an element of discovery in terms of what was going over the wire that helped me visualize potential threats or hot spots I didn't necessarily anticipate," says Rahbany.

DON'T forget proprietary applications. These are not the apps you're going to be watching for unauthorized activity—at least not through your firewall—but you want to make sure you do no harm.

"It's a bit of a weak link for a lot of vendors," says Phifer, "Most have some methodology for identifying them." She recommends taking a sampling of proprietary applications, crafting rules and policies, and finding out whether there is a risk of blocking legitimate apps or generating false positives. ■

Neil Roiter is a frequent contributor to CSO. Send feedback to editor Derek Slater at dslater@cxo.com.

Are You an IT Security Leader?

An astonishing number of survey respondents believe they are IT security leaders. But what does it really take to be a leader, and how does your organization stack up? **By George V. Hulme**

A surprisingly high—unreasonably high, in fact—number of organizations think their security program is part of the vanguard of risk management.

That was one surprising finding of this year's annual Global Information Security Survey, conducted by *CSO* and *CIO* magazines in partnership with PricewaterhouseCoopers. More than 9,600 business and technology executives from around the world took the survey, and 43 percent of those surveyed believe their organizations are IT security leaders. The other categories respondents could choose from were strategist, tactician and follower.

Obviously those enterprises, by definition, can't *all* be at the forefront of security. "Most of these 'leaders,' in my opinion, have a false sense of their level of security," says Mark Lobel, a principal in the advisory services division of PwC.

Ahead of the Bell Curve

In an attempt to identify the organizations that might actually be information security leaders, PwC filtered the results according to conditions it felt would qualify a company to deserve the label.

- First, the CISO had to report directly to a senior executive.
- Second, the organization had to have an IT security strategy in place and the ability to execute that strategy.
- Third, it had to have reviewed its security policy in the past year.
- And finally, if the company had suffered a data breach, it had to know the breach's cause.

Under those criteria, less than 5 percent of respondents' organizations actually made the cut.

About half of respondents reported suffering one or more breaches, and a third said they weren't breached in the past year.

About 8 percent couldn't tell whether they had been breached or not. The good

43%

believe their organizations are IT security "leaders"

news from those figures is that a growing number of companies believe they understand the security events happening on their networks, and know what applications or systems were infiltrated.

However, that confidence doesn't align with the increased sophistication of malware in recent years. "In our engagements and my conversations with peers, we are dealing with more organizations that are grappling with international infiltration," says Shawn Moyer, practice manager of research consulting at Accuvant Labs.



(For more on this topic, see "Customized, Stealthy Malware Growing Pervasive" at www.csoonline.com/article/677541). "Every network we monitor, every large customer, has some kind of customized malware infiltrating data somewhere," Moyer says.

"I think there are a lot of executives out there with a false sense of security," says one security manager at a Midwest manufacturing firm. "In our company, many upper managers simply choose to believe the reports that come in from the different regions. If those reports say that the systems are tight and secure, then that is management's working assumption."

So it seems many organizations are overconfident about their security posture. What attributes, then, does an IT security program need to have to truly be ahead of the pack?

85% employ a CISO or CSO

"From a maturity perspective, if you have a senior manager or a junior executive who is designated as a security lead, that's my number-one criterion," says Eric Cowperthwaite, CSO at Providence Health and Services. Before you can consider your organization on the leading edge, "you have to have a security front-person, who's recognized as such in your organization, and is high enough up in the organization to have actual authority," he says. "Number two is to have a strategy, not just a road map for

what technologies you are going to deploy, but a strategy for how you are going to secure and protect your systems and data," Cowperthwaite adds, an assessment that largely parallels PwC's definition.

The semantics of titles aren't a major concern. Andy Ellis, CSO at Akamai Technologies, says, "I don't think it matters what title you have. What matters is that you are efficiently reducing your risk according to your organization's business requirements."

That's hard to argue against, but few survey respondents could pass Ellis' litmus test because so few are actually testing their security efforts. Consider this: While 63 percent of respondents have an overall IT security strategy and 85 percent employ a CISO or CSO, half or less of those surveyed

LAGGARD TO LEADER: WHAT IT TAKES TO GET THERE

What are the best ways for strategists, tacticians and followers to become IT security leaders with mature processes?

How do organizations move from lagging in their IT security program to leading? They must put an effective strategy in place, consistently meet that strategy, and have good visibility into the security events in their infrastructure. Looks good on paper, but how do you get there? CISOs say it boils down to executive vision and support.

However, according to the survey responses, security professionals are focused more on technologies and less on integrating security processes throughout the business.

For instance, only 48 percent report linking security, via organizational structure or policy, to privacy or regulatory compliance. And only 46 percent employ dedicated security personnel who support internal business departments.

Those are just two examples of the disconnect. Others include not aligning security spend with real-world business risk and not having healthy lines of communication with executive leadership. Part of the problem, security industry experts say, is of IT security's own making. "Many security professionals do not behave as if they are a critical business function. Instead of discussing business risk, they discuss attack techniques and technologies," says Eric Cowperthwaite, CSO at Providence Health and Services.

That communication problem, says Daniel Kennedy, research director for information security and networking at the research firm TheInfoPro, is largely a by-product of an old story: Organizations promote highly technical personnel to what should really be a business-management role.

"They figure, 'That's the person who managed the firewall, therefore let's

make them the CISO,'" says Kennedy.

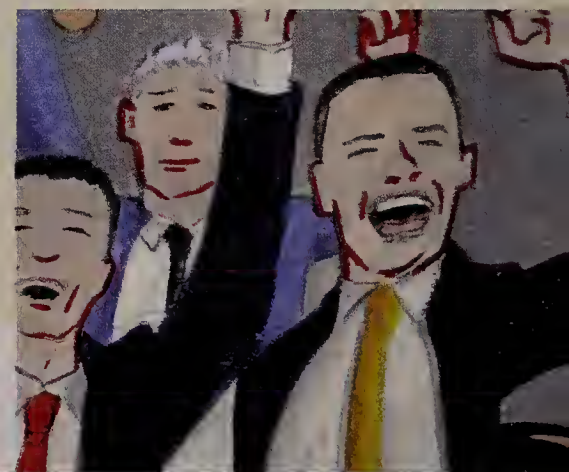
"There has to be some consideration that there are people out there who are good communicators, good senior executives, and then there are people for whom that's not in line with their capabilities," he says.

"I speak with other companies all the time, and there are many CISOs with that title, but their real strategy is to make their firewalls run better, so they're always working at a low tactical level," says Providence Health's Cowperthwaite.

That means to move from laggard to leader, more enterprises need to elevate the CSO position from a tactical level to the level of a business risk adviser.

TheInfoPro's Kennedy says that to get there, the first step is to build credibility.

"If management doesn't trust the CISO, then they don't have the right guy. The security leader is someone functioning on the executive level, someone who



50% or less

are actively
evaluating their
security efforts

are evaluating their efforts. For example, while 63 percent said they have an overall information security strategy, about 40 percent said they've established security baselines for external partners, and only 43 percent have centralized security informa-

tion management processes. Similarly low percentages of survey-takers have identity-management strategies (41 percent), business-continuity or disaster-recovery plans (39 percent), or risk-based authentication systems (34 percent).

Business Impact

Companies that don't have a security leader, a strategy, and the ability to execute that strategy and measure their execution are likely to suffer more breaches than others—that seems obvious. But they may also be losing more business.

That's the argument made by Douglas Davidson, president and CEO of security services provider Jacadis. "Clearly, they miss [business] opportunities. We have small businesses that we work with that have been driven to follow a [standards]-

About 8%

couldn't tell
whether they had
been breached in
the past year

based security program by their bigger customers and business partners. They've actually gained revenues because they've created a competitive advantage through the security they put in place," he says.

How can security drive revenue? By using secure processes to gain partner and customer trust, and even to deliver new services to clients. Davidson cites a recent example: "There were several banks that needed the ability to send paper statements for printing, but most of the printers in the area were not able to secure the necessary processes. This one printer was able to build proper security around their services. They then won the banks' business and were able to go out and sell that capability to other customers," Davidson says.

That anecdote shows that IT security isn't a discipline practiced within a business; it's an integral part of the business. "For any significantly sized company, information security is a critical business function because information management is a critical business function," says Cowperthwaite.

Now if only more businesses would act as if IT security is critical to their business—or at least live up to their own mental images of their security efforts. ■

George V. Hulme is a security and technology writer based in Minneapolis. Send feedback to editor Derek Slater at dslater@cxo.com.

Watch for our next issue
for more survey findings,
including data about specific
gaps in prevention programs.

can speak IT in business terms, and somebody who really effects cultural change in the company," he says. "That means there should be a difference between the day they started and a year and a half later in terms of the way the company views security. If they're not getting that, you don't have a security leader. What you have is somebody who is sort of just sitting around in the role," says TheInfoPro's Kennedy.

That trust, in combination with executive leadership, will go a long way toward getting the security budget and resources needed to build a solid program.

But it's not enough. Experienced pros say that the CISO who can build a world-class program has to first be an expert on the industry they're in and how their organization functions in that industry. That's why Cowperthwaite advises CISOs to learn the nature of their business. "If you want to be the CISO of the company, then somebody else can go talk about bits and bytes with your networking equipment provider while you figure out what the company's strategy is and how you fit into it," he says. "You can do that better by getting to know the business inside out," he says. "If you work in

transportation, you have to go out in the road with the drivers. See how everyone works and what they need to get their jobs done. If you're a hospital, watch how staff actually works."

Finally, to be security leaders, enterprises need to start measuring their efforts so that they can improve over time. Pete Lindstrom, research director at Spire Security, says a good place to start is with operational metrics. Those would include commonly repeated tasks such as user provisioning, account management, and time from vulnerability discovery to remediation. The measurements can also be risk-based, such as vulnerability-management efforts. "The important thing is to start measuring what you can measure, and build the metrics you can track over time," Lindstrom says.

While most organizations still lack a cohesive security strategy and an ability to execute on that strategy, it's clear that it's not beyond their reach to develop those things. Security management needs to be in a position of authority, integrate itself into the business and continuously measure and improve upon its own efforts. —G.V.H.



Facial Recognition and Social Media Meet in the Shadows

Starting with just a Facebook profile photo, researchers obtain partial Social Security numbers and other sensitive information. Richard Power interviews Alessandro Acquisti.



FACEBOOK WILL LIKELY reach one billion users this year or next.

The privacy and security implications of this astonishing amass-

ing of personal information are mind-boggling.

Imagine having access to the political views, sexual preferences, relationships, tastes, foibles, emotional states and workplace attitudes of a billion people.

An effort to collect such data on behalf of a government, or a corporation, or a geopolitical alliance, or an industrial sector, or even a seemingly benign world organization would meet with fierce opposition. It would be difficult, if not impossible; it would require lawyers, money and maybe even guns.

But in the era of social media, an extraordinary and rapidly growing number of us have been willingly posting such sensitive information (or at least the keys to unlocking it) online, where it's available either directly or indirectly to marketers, stalkers, reporters, law enforcement, private investigators, human resources personnel and rivals in love, business or politics, whether it's obtained by subterfuge or inference or subpoena, whether legally or illegally, whether ethically or unethically.

It is all out there now, and not just spread across cyberspace in fragments. No, it's happily, willingly offered up in an organized way.

Consider, for example, the Facebook profile photo.

No matter how tightly you zip up your Facebook account,

SOCIAL NETWORKING

people who you have not friended can see your profile photo. And isn't that the point for most of us—not just to share status updates, photos, videos, likes and comments with our current circle of friends and colleagues, but to expand that circle?

But what if a stranger on the street could snap a smartphone photo of you, and then use facial-recognition software to match it to a profile photo on Facebook, and then learn your name and your date of birth, who's in your circle of friends, and other such data?

What if that stranger could then take some of that data and guess your Social Security number from it, granting them unrestricted access to the most sensitive details of your financial and medical information?

Well, it is possible, as *The Economist* (which broke this story) recounts:

"By mining public sources, including Facebook profiles and government databases, the researchers could identify at least one personal interest of each student and, in a few cases, the first five digits of a social security number. All this helps to explain concerns over the use of face-recognition software by the likes of Google and Facebook, which have been acquiring firms that specialize in that technology, or licensing software from them. (Google recently snapped up Pittsburgh Pattern Recognition, the firm which owns the programme the researchers used for their tests.) Privacy officials in Europe have said they will scrutinise Facebook's use of face-recognition software to help people 'tag,' or identify, friends in photos they upload. And privacy campaigners in America have made a formal complaint to regulators. (Facebook notes that people can opt out of the photo-tagging service by altering their privacy settings.)"

Yes, Alessandro Acquisti and Ralph Gross, the two Carnegie Mellon University researchers who rocked the world a couple of years ago with their blockbuster study proving that Social Security numbers could be guessed, have done it again.

The experiment that yielded the information on a study subject's Social Security numbers was the third of three experiments.

The first experiment was about online-to-online re-identification. The researchers



"When I can recognize your face in the street, using a face recognizer, and also find your Facebook profile that way, I can not only identify you, but also infer additional sensitive information about you."

—ALESSANDRO
ACQUISTI

showed that they could identify a significant proportion of users of a popular dating site by taking unidentified profiles from the site (where people use pseudonyms to protect privacy) and comparing them, using facial recognition, to identified profiles on Facebook (without even logging onto the network itself; they simply used the parts of the Facebook profiles they could see using a search engine).

The second experiment was about offline-to-online re-identification. It was conceptually similar to the first experiment, but the researchers tried to identify students on the Carnegie Mellon University campus after taking three shots of them

with a cheap webcam. It took on average three seconds to identify more than 32 percent of the students photographed.

Acquisti, one of the co-authors of the study, presented the results of the study at Black Hat Briefings (where else?) on Aug. 4. Acquisti is a colleague of mine at Carnegie Mellon University CyLab, an advanced academic research program exploring 21st Century cybersecurity and privacy. He is also an associate professor of information technology and public policy at Carnegie Mellon's Heinz College.

We recently sat down to conduct this interview for the readers of CSO.

Power: Tell us about this study. How did it come about? What are the intersecting trends that drew you and your co-researchers to look into this issue?

Acquisti: We actually started thinking about this study six years ago. Ralph Gross and I had written what turned out to be the first peer-reviewed published article about Facebook ("Information Revelation and Privacy in Online Social Networks"). Facebook was very young at the time, but its members were already revealing lots of personal information, and in particular, identified primary profile photos. We thought that this could lead to visual re-identification, but we only started serious work on this idea after completing another one of our studies, the one about predicting Social Security numbers from public data, including, in fact, Web 2.0 profiles.

In your presentation, you mention that Facebook may be evolving into a default real ID. Explain.

Facebook users tend to create profiles under their real first and last names. This is due to a combination of reasons. First, when Facebook started, it was a campus-based social network, where members felt they shared something in common. Therefore members felt more comfortable using their real identities, as compared to behavior on MySpace or Friendster at the time. Of course, that Facebook community is in reality very much open—we call it an imagined community in one of our papers. Second, as Facebook expanded outside college networks, it realized that forcing a verified identity policy was good business; it meant better data on members and consumers. As

a result, according to some of our estimates, about 90 percent of Facebook users use their real identities on the network. If you combine this fact with another one—that the vast majority also use frontal face photos of themselves as their primary profile photos (which, by the way, Facebook makes visible to all by default)—you end up with a de facto real ID.

Tell us what you mean by “augmented reality” and what this research shows us about its consequences and implications?

We use the term “augmented reality” in an expanded sense, to refer to the merging of online and offline data that new technologies make possible. When I can recognize your face in the street, using a face recognizer, and also find your Facebook profile that way, I can not only identify you, but also infer additional sensitive information about you (such as, in our third experiment, your Social Security number). Essentially, we start from an anonymous face in the

street, and we end up with very sensitive information about that person. This is the kind of future we are walking into whether we like it or not, and the consequences and implications of this seamless blending of online and offline data are anybody’s guess.

You also mentioned scalability issues in your presentation. In what ways may scalability affect this trend?

As of today, automated face recognition is still pretty bad, but it keeps improving. If you look at the technological trends in cloud computing, the accuracy of face recognizers, and online self-disclosures, it is hard not to conclude that what we present today as a proof-of-concept in our study will tomorrow become as common as everyday text-based searches on a search engine.

What are the immediate or near-term implications of this study for users of Facebook and social media, both personally and professionally? And likewise, what are the

immediate or near-term implications for organizations in regard to their workforce? What do governments and advocacy groups need to get their minds around in regard to these technological capabilities?

There is no obvious answer or solution to the privacy concerns raised by widely available facial recognition. Google’s Eric Schmidt observed that, in the future, young people may be inclined to change their names to disown youthful improprieties. It is much harder, however, to change someone’s face. Other than adapting to a world where every stranger in the street could quite accurately predict your credit score and sexual orientation, we need to think about policy solutions that can balance the benefits and risks of peer-based facial recognition. Self-regulation is not going to work. ■

Richard Power is a Distinguished Fellow at Carnegie Mellon CyLab. Contact Editor Derek Slater at dslater@cxo.com.

Enroll now.

**ON THIS BATTLEFIELD,
EDUCATION IS YOUR BEST DEFENSE.**

Cyber attacks are being waged all over the world, creating an unprecedented demand for trained professionals to protect our country’s data assets and develop cybersecurity policies. Help meet the demand with a bachelor’s or master’s degree in cybersecurity. Whether you plan to work for Cyber Command taking down cyber terrorists or for private industry battling hackers, UMUC can help you make it possible.

- Designated as a National Center of Academic Excellence in Information Assurance Education by the NSA and DHS
- BS and MS in cybersecurity and MS in cybersecurity policy available
- Programs offered entirely online
- Interest-free monthly payment plan available, plus financial aid for those who qualify

CYBERSECURITY

800-888-UMUC • umuc.edu/cyberspace

 **UMUC**
University of Maryland University College
Copyright © 2011 University of Maryland University College

[INDUSTRY VIEW]

By Frank Villavicencio, EVP, Identropy

Top 10 Identity-Management Metrics that Matter

Within the IT security community, identity- and access-management (IAM) initiatives are considered high value, but are notoriously problematic to deploy. Yet despite IAM's complexity, it represents 30 percent or more of the total information security budget of most large institutions, according to IDC (a sister company to CSO's publisher).

Ironically, the deployment difficulties stem from having to reconcile the very people and process breakdowns IAM automation is meant to solve, such as too many or too few people involved in authorizing requests, a lack of documentation for access requests and approvals, connecting to target systems with "dirty" or obsolete data, and so on. This conundrum has led to the rise of what is called identity governance.

Identity governance involves defining and executing the identity-related business processes that are most critical to the organization. For example, an engineer needs root access to the server hosting an ERP system—who needs to approve that request? Who is the one who actually takes the action that grants that access? How does that process get documented? Where is it stored, and for how long? How can we report on it during an audit?

Getting your organization's governance processes locked in is a tall order, but well worth it. One of the many benefits of proper identity governance is that it pinpoints which identity-related processes are most in need of attention. Here are 10 of the most common measurements for gauging the effectiveness of identity governance.

1. Password reset volume per month. This one is a classic in identity manage-



ment, and it's key to helping organizations measure the effectiveness of their IAM programs. Businesses typically look at password-related help desk calls, account lockouts, and self-service resets per month as good indicators of password-policy effectiveness. This metric should generally trend downward, although there may be peaks and valleys driven by business events. If it doesn't, your organization's password policies and management tools require a closer look.

2. Average number of distinct credentials per user. Another IAM classic, and for years, a key business justification for single sign-on (SSO) initiatives. The industry average ranges from 10 to 12 unique accounts per user. Organizations should strive to bring this average down as close to one as possible.

3. Number of uncorrelated accounts. These are accounts that have no owner, and occur most frequently when a change hap-

pens, such as a promotion or a termination, and that person's accounts were not transitioned properly. Too many uncorrelated accounts can lead to unnecessary risks—they are open, live accounts that can be easily hijacked for unauthorized use.

4. Number of new accounts provisioned. This number should closely follow the number of new joiners to the organization. An effective IAM program should always account for any new user who needs to be granted access to systems and applications. If there's

a discrepancy or a significant lag between the number of provisioned accounts and the total number of new joiners for a given period, that indicates inefficient processes or poor identity data.

5. Average time it takes to provision or de-provision a user. This shows how long a new user waits to get access to the resources they need to do their work. It has implicit productivity and ROI ramifications. Nine times out of 10, if someone doesn't get access to applications in a timely fashion, there are process issues behind the delay. This metric can flag a business process that needs to be reviewed and possibly adjusted.

6. Average time it takes to authorize a change. This metric can provide insight into the efficiency of an organization's approval processes. For example, if there are four people involved in approving a sales rep's access to Salesforce.com, but it takes two weeks for that approval to be granted, that's

two weeks the sales rep is limited in his capacity to sell. Knowing how long it takes for approvals to be granted can help identify bottlenecks or out-of-date processes.

7. Number of system or privileged accounts without an owner. These are also known as orphaned accounts. They crop up when people who had the credentials to grant them access to important resources—making them privileged users—no longer need access to those resources but never had their privileges removed. This problem here is obvious—who wants privileged accounts that don't belong to anyone floating around?

8. Number of exceptions per access re-certification cycle. A high number of exceptions is expected for new applications or user sets being brought under governance, but over time this should trend toward zero. A consistently high number of exceptions is a strong indicator of poor identity data quality (that is, lots of users having access that they should not have), or of process

problems (that is, the person requesting re-certification does not have all the information they need to complete the process.)

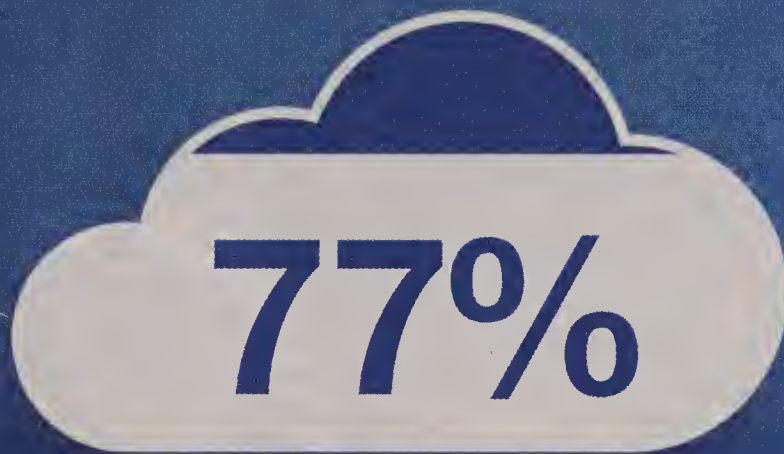
9. Number of reconciliation exceptions. Reconciliation exceptions are typically caused by the inability of an IAM platform to reliably tie an identity to an account in a target system. This is usually the result of manual entry errors (that is, user names or unique identifiers are not matched), or worse yet, of an account created by back-door channels. These exceptions should trend toward zero over time, and any spikes should trigger a thorough investigation and further discussion.

10. Separation of duty violations. Examples of separation of duty violations include developers who have admin access to production databases and traders who can submit and approve their own transactions. These are more difficult to catch and measure, given their sophistication and cross-application nature, but are also the riskiest to miss, given the potential

damage that could be inflicted if they're exploited. Exploitations of these problems are the kind that often make headlines. The organization should implement preventive controls to monitor these violations, report them and orchestrate their remediation.

It's often hard to understand the scope and ramifications of these kinds of people and process breakdowns until you take concrete steps to address them. That is part of the reason IAM and identity governance are perceived as daunting and, at times, painful. But only with metrics can the organization measure its effectiveness and success in efficiently managing user access, and make the necessary adjustments to reap significant security, compliance and operational benefits. If you have started an identity governance initiative, do your best to track some of these metrics—you'll be glad you did. ■

Frank Villavicencio leads Identity's Managed Identity Services business.



**of FORTUNE 500s Rely On Box®
Including Dell, P&G and Clear Channel**

Secure content sharing and collaboration
that users and IT love and adopt.



Get the Box CSO Tool Kit at Box.com/CSO

[DEBRIEFING]

Welcome to UltraCorp

A few friendly reminders from Team Security for the recent college grads in our workforce



Hello and congratulations on completing your six-month new-employee probationary period. We'd like to take this opportunity to answer some of your questions and respond to some of your suggestions from the employee survey.

1. With some reluctance, in response to user request we are looking into the possibility of creating a first-person-shooter-style iPad app you can use for filing your reports of parking lot vehicle damage.
2. Finance rightly refused to allow smartphone access to the core ERP modules. They've indicated they'll put it all into Amazon AWS public cloud anyway; we look forward to continuing our discussions with them about that.
3. To the R&D group—we admire and appreciate your enthusiasm for that next-generation product you're working on. However, you must immediately remove the meeting notes from the Facebook page you created. Yes, even though you have 1,306 likes already.
4. As for those two clever tricks you "invented" (as several of you characterized it in your UltraCorp Newbie LinkedIn group. Yes, we can read that.) for helping friends who've forgotten their access cards: Passback and tailgating have been around for decades.
5. We were surprised to find usage of freelargefiletransfer.com has spiked in several departments since your arrival. We spent a good deal of money (er, "bread") last fiscal year installing a secure, encrypted file-transfer program that integrates with our email system. ("Email" is a messaging program. It's a lot like Twitter, only turn-based instead of real-time.) Could you pretty, pretty, pretty, pretty please use that instead?

Your required cooperation is appreciated,
Team Security

x.4213

P.S. Follow us on Twitter! @teamsecurityultracorp

LEGAL NOTICE

U.S. POSTAL SERVICE STATEMENT OF OWNERSHIP, MANAGEMENT and CIRCULATION (Required by 39 U.S.C. 3685)

1. Title of Publication: CSO
2. Publication No.: 021-412
3. Date of filing: September 12, 2011
4. Frequency of issue: 10 issues yearly with a combo Dec/Jan and Jul/Aug
5. Number of issues published annually: 10
6. Annual subscription price: Free to qualified subscribers/All other in U.S. and Canada \$70.00; Foreign Subscriptions, \$95.00 USD.
7. Location of known office of publication: 492 Old Connecticut Path, PO Box 9208, Framingham, MA 01701-9208 (Middlesex-Central County).
8. Location of the headquarters of general business offices of the publishers: CXO Media, 492 Old Connecticut Path, PO Box 9208, Framingham, MA 01701-9208 (Middlesex-Central County).
9. Names and addresses of the publisher, editor and managing editor:
Publisher, Bob Bragdon, 492 Old Connecticut Path, Framingham, MA 01701-9208.
Editor-in-Chief, Derek Slater, 492 Old Connecticut Path, Framingham, MA 01701-9208.
Managing Editors, Bill Brenner, and Joan Goodchild, 492 Old Connecticut Path, Framingham, MA 01701-9208.
10. Owner: International Data Group, 1 Exeter Plaza, Boston, MA 02116-2851.
11. Known bondholders, mortgages and other security holders owning or holding 1% or more of total amount of bonds, mortgages or other securities: International Data Group, 1 Exeter Plaza, Boston, MA 02116-2851. None
12. For completion by nonprofit organizations authorized to mail at special rates: Not applicable.
13. Publication Name: CSO
14. Issue date for circulation data below: September 01, 2011.
15. Extent and nature of circulation:

	Average No. Copies Each Issue during Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
A. Total number of copies printed (net press run)	29,336	29,687
B. Legitimate paid and/or requested distribution (by mail and outside the mail)		
1. Outside county Paid/Requested mail subscriptions stated on PS Form 3541	28,521	28,521
2. In-county paid/requested mail subscriptions stated on PS 3541	0	0
3. Sales through dealers and carriers, street vendors, counter sales, and other non-USPS paid distribution	65	52
4. Requested copies distributed by other mail classes through the USPS	0	0
C. Total paid and/or requested circulation	28,586	28,573
D. Nonrequested distribution (by mail and outside the mail)		
1. Outside county nonrequested copies stated on form 3541	0	0
2. In-county nonrequested copies stated on form PS 3541	0	0
3. Nonrequested copies distributed through the USPS by other classes of mail	0	0
4. Nonrequested copies distributed outside the mail	762	1101
E. Total nonrequested distribution (Sum of 15d (1), (2), and (3))	762	1101
F. Total distribution (Sum of 15c and 15e)	29,348	29,674
G. Copies not distributed	0	0
H. Total (Sum of 15f and 15g)	29,348	29,674
I. Percent paid and/or requested circulation (15c/15f x 100)	97.4%	96.3%

I certify that the statements made by me above are correct and complete.

Diana Turco
Diana Turco
Circulation Manager

cloud security. can you see beyond the problem? you can

The #1 issue for companies migrating to the cloud is identity and access management. But for the agile business, *know*-ing users is always better than *no*-ing them.

In fact, agile businesses, using our Content-Aware Identity and Access Management solutions, have been able to reduce security risk while improving productivity, access and efficiency. More effective compliance, reduced IT risk, broader, more secure customer and partner relationships.

That's what happens when *no* becomes *know*. And security turns into agility.

To see how we can help make your business more agile and secure, visit ca.com

ca world '11

register today
ca.com/caworld

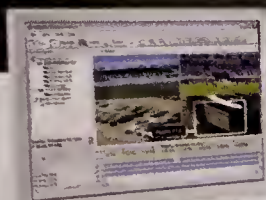
IT at the
speed of business

agility
made possible™

ca
technologies



CAPTURE IT WITH CLARITY



**Avigilon's end-to-end surveillance solutions
give you image detail no other system can match.**

Get unprecedented clarity with the Avigilon Control Center software featuring High-Definition Stream Management (HDSM) technology, and the broadest range of megapixel cameras – from 1 to 29 MP. Our scalable surveillance solutions require minimal bandwidth and storage while producing the very best image quality. And that means you always get the best evidence.